(U) Continuous Monitoring Capability (CMC)

An Enterprise Fit

(U) Stephen G. York
Enterprise IA Architecture and Engineering Services
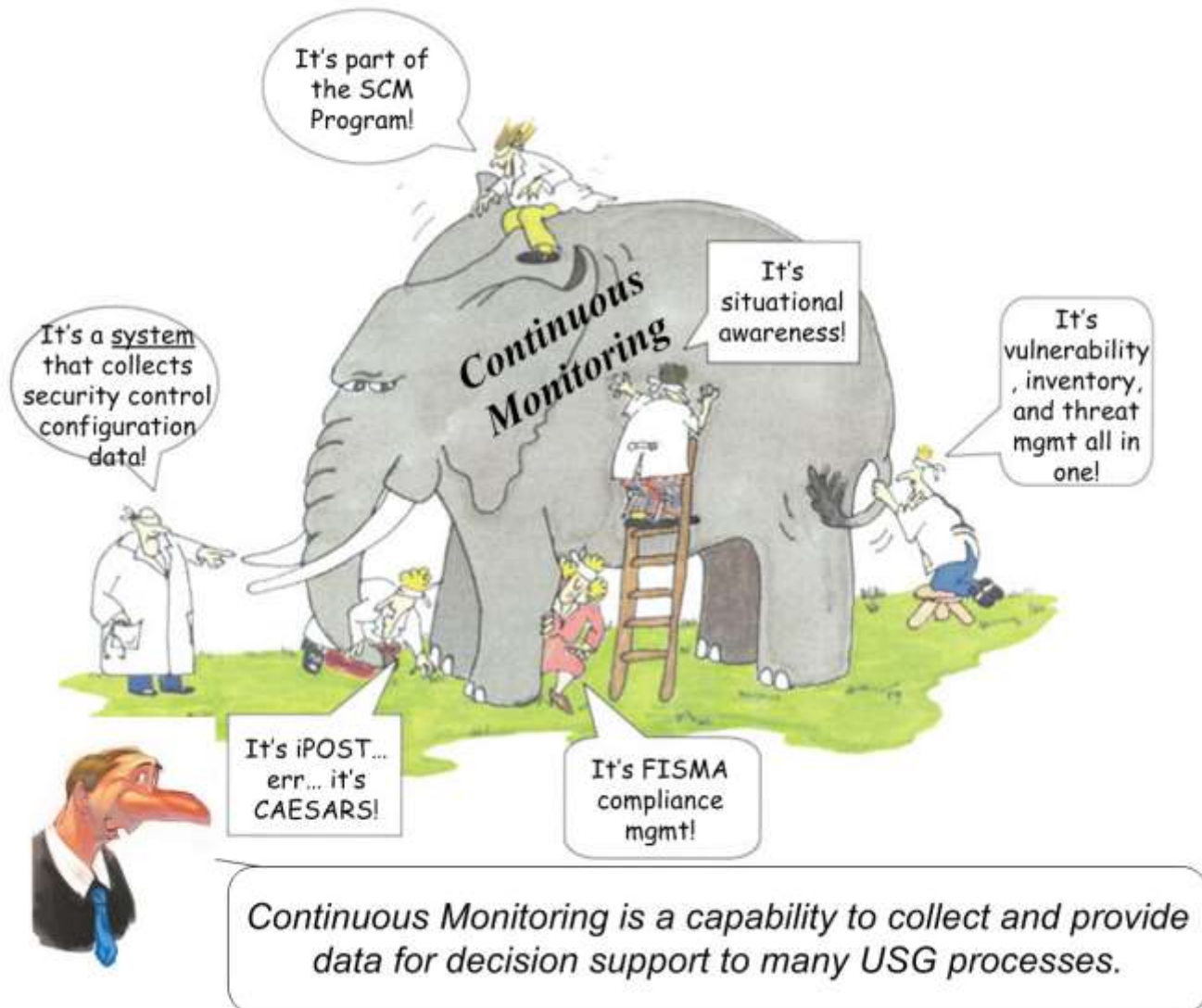**March 2011**

(U) Agenda

(U) Continuous Monitoring Capability (CMC)
- Multiple Views
- Unified View
- Definitions
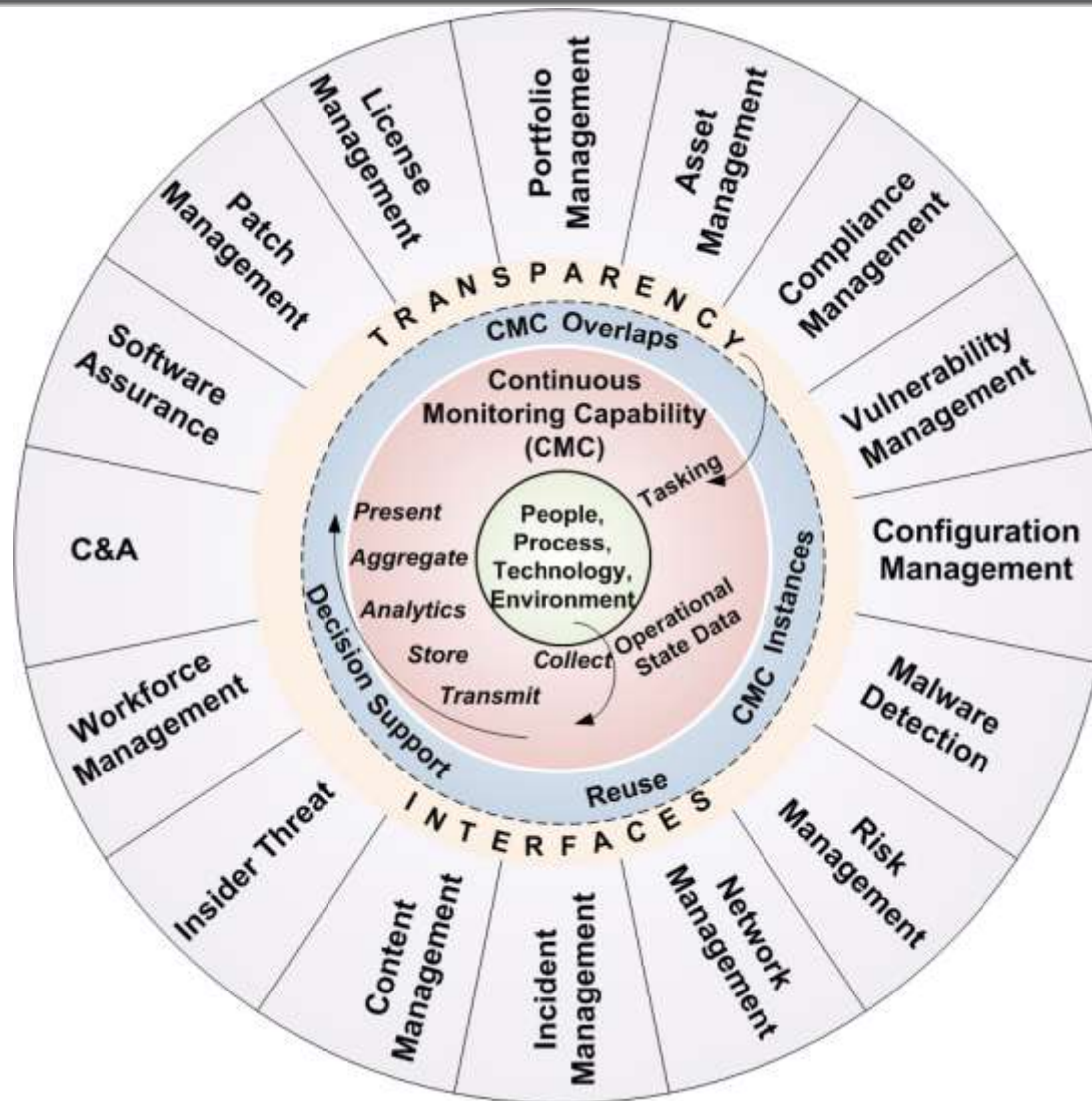- Intent
- Organizational Scope

(U) Multiple Views

(U) Unified View

(U) Definitions

(U) Continuous Monitoring
- On-going observance with the intent to provide awareness.

(U) USG Continuous Monitoring Capability
- On-going observance of operational states to provide a unified view for operations and compliance decision support.

(U) Information Security Continuous Monitoring
- Awareness of information security status to support organizational risk management decisions.

(U) *<Your Qualifier>* Continuous Monitoring
- Specific to your decision support needs

(U) Intent

(U) Continuous Monitoring Intent

- <u>enabling efficiencies</u> surrounding a unified view for operations, readiness, and compliance decision support; doing what we do today better, faster, cheaper

- Present data/results to provide decision support for many USG functional areas including, but not limited to:
- OMB via Cyberscope to provide FISMA compliance status
- USCC via DISA to support situational awareness
- Operations mgmt to support SOE compliance
- Intelligence analysis to provide adversary presence awareness
- Patch levels in support of Patch Mgmt process

The combination of *your* definition and the intent is what communicates the scope and purpose

(U) Efforts and Successes

(U) Dept of State – iPost
• Demonstrated capability – 94% increase in network security posture
• Changed a culture: awareness and accountability regarding security

(U) Dept of Homeland Security
• Oversight and coordination
• CAESARS architecture
• Established USG level working group

(U) Information Security and Identity Management Committee (ISIMC) Continuous Monitoring Working Group (CMWG)
• Supports all USG agencies
• CAESARS architecture – Implementation Reference Architecture
• Improve FISMA metrics for upcoming years
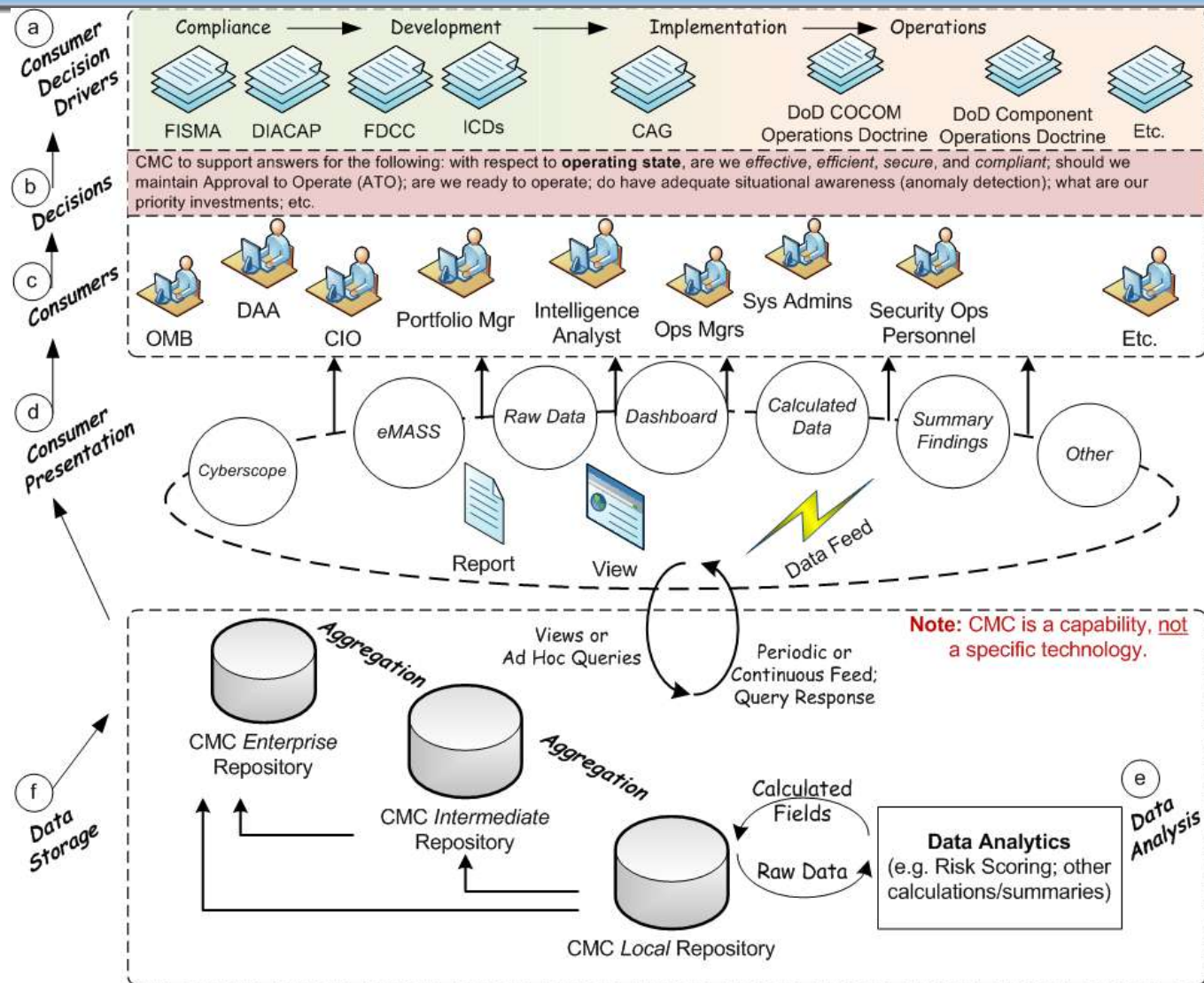• Technology transfer between DOD and Civilian Departments and Agencies
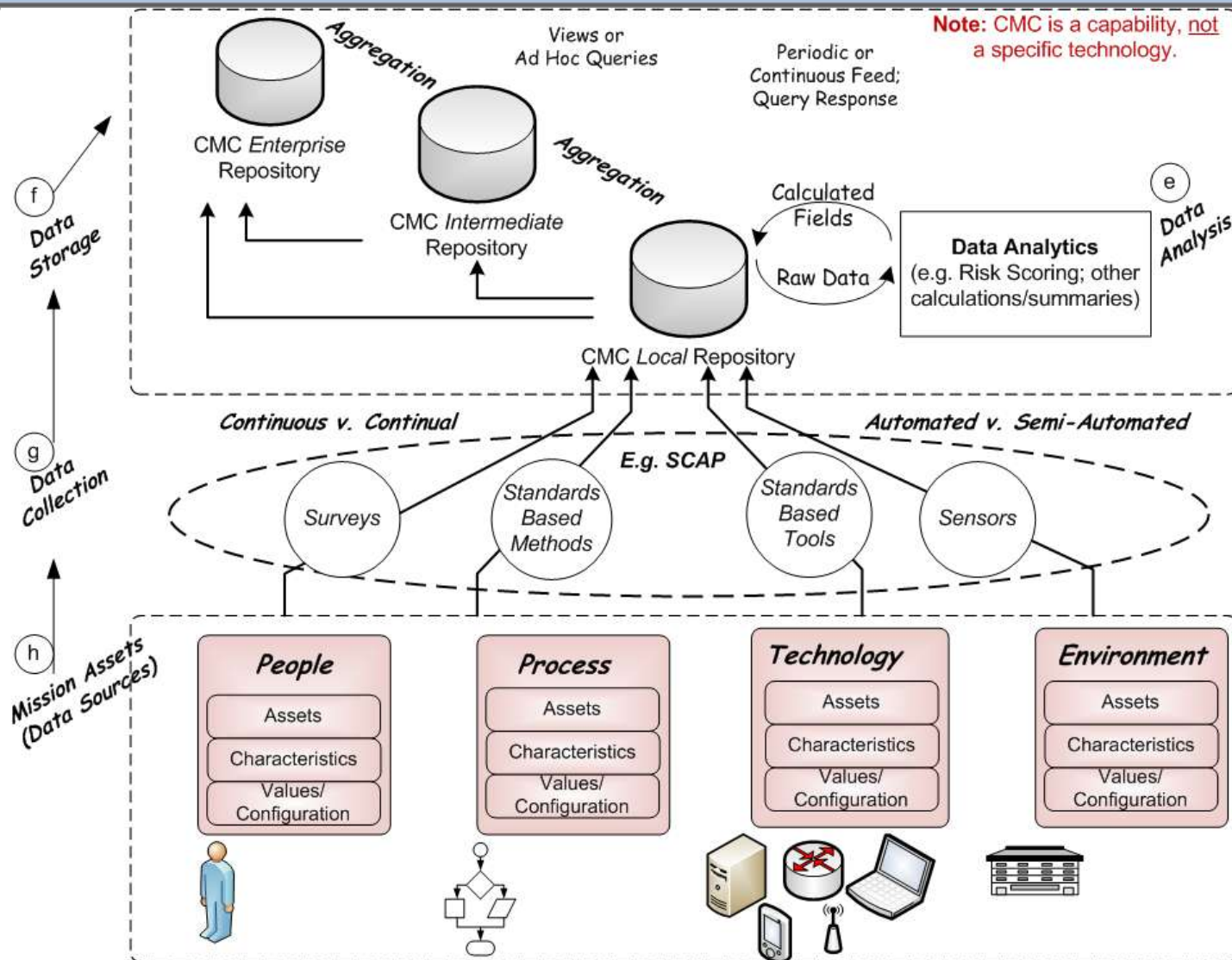
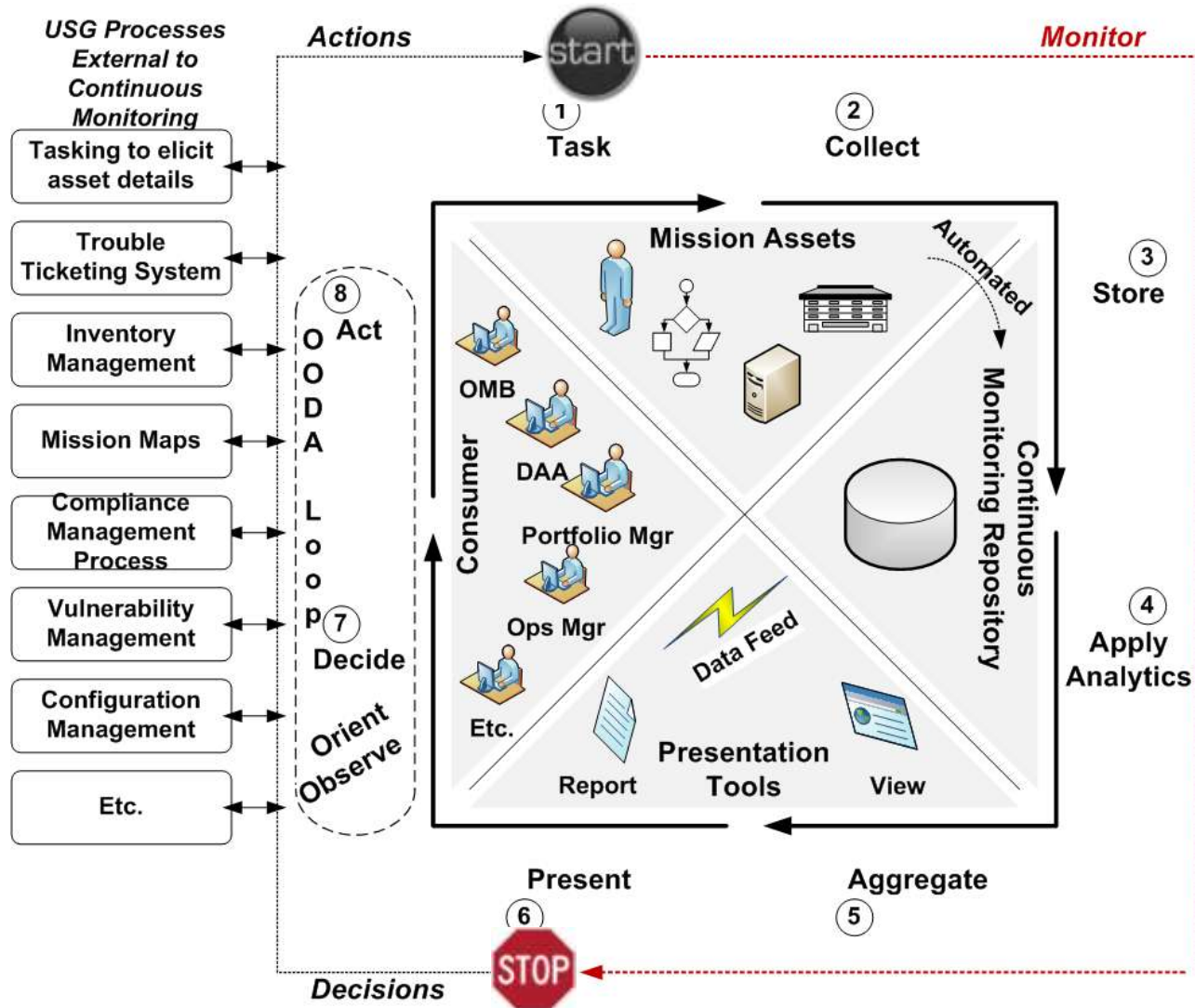# (U) Enterprise Architecture
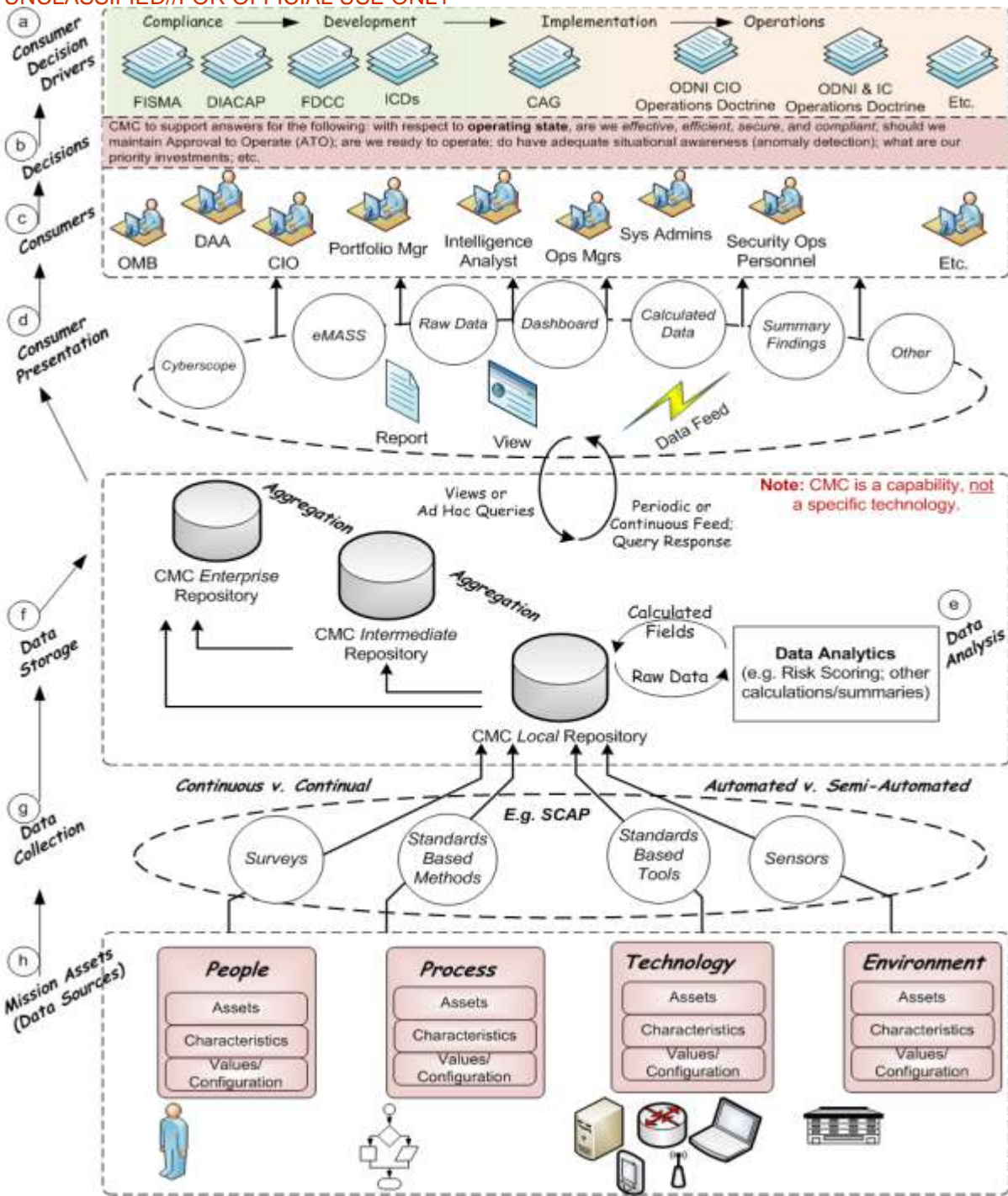
(U) Consumer Perspective

(U) Provider Perspective

(U) CMC Workflow

(U) Questions?